UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,291	08/16/2001	Marinus Frans Kaashoek	12221-005001	3137

26161 7590 10/01/2004

FISH & RICHARDSON PC
225 FRANKLIN ST
BOSTON, MA 02110

EXAMINER	
JACKSON, JENISE E	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/931,291	KAASHOEK ET AL.	
	Examiner	Art Unit	
	Jenise E Jackson	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-6, 9-13, 15-16, 20 remain rejected under 35 U.S.C. 102(e) as being anticipated by Porras et al(6,321,338).

3. As per claim 1, Porras et al. discloses a central control center(i.e. resolver, ref #20, fig. 2, sheet 2) to coordinate thwarting attacks(see col. 7, lines 43-54, col. 13, lines 31-59) on a victim data center(i.e. domain)(see col. 3, lines 17-21, 32-35, col. 8, lines 31-45, that is coupled to a network(see col. 8, lines 66-67), a communication device to receive data from a plurality of monitors, dispersed through the network, the monitors sending data collected from the network(see col. 2, lines 36-53, col. 5, lines 4-22), over a hardened, redundant network(see col. 8, lines 13-21); a computer system, the computer system includes, a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic(see col. 13, lines 16-30).

4. As per claim 2, Porras et al. discloses an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center(see col. 5, lines 4-22, col. 13, lines 60-65, col. 14, lines 1-7).

5. As per claim 3, Porras et al. discloses wherein the data analyzed by the control center is collected statistical information about network flows(see col. 2, lines 36-53).

6. As per claim 4, Porras discloses aggregates traffic information and coordinates measures to locate and block the sources of an attack(see col. 1, lines 55-65, col. 5, lines 4-22).

7. As per claim 5, Porras discloses wherein the control center is a hardened site(see col. 2, lines 8-10).

8. As per claim 6, Porras discloses wherein the monitors include gateways that are disposed at the victim data center and data collectors that are disposed in the network(see col. 2, lines 8-53, col. 3, lines 66-67, col. 4, lines 1-17) the analysis process executed on the control center analyzes data from gateways and data collectors dispersed throughout the network(see col. 8, lines 13-30).

9. As per claim 9, it is rejected under the same basis as claim 1.

10. As per claim 10, limitations have already been addressed(see claim 2).

11. As per claim 11, limitations have already been addressed(see claim 4).

12. As per claim 12, Porras discloses receiving and analyzing are performed by a control center coupled to the data collectors via the hardened, redundant network(see col. 8, lines 13-21).

13. As per claim 13, Porras discloses wherein plurality of monitoring devices(see col. 8, lines 13-21); are data collectors dispersed throughout the network and at least one gateway device that is disposed adjacent the victim site to protect the victim)(see col. 3, lines 17-21, 32-35, col. 8, lines 31-45), and wherein analyzing includes analyzing at a control center data from the at least one gateway and the data collectors dispersed throughout the network(see col. 8, lines 13-30).

14. As per claim 15, it is rejected under the same basis as claim 8.

15. As per claim 16, Porras discloses sending requests to gateways and/or data collectors to send data pertaining to an attack to the control center(see col. 8, lines 40-46).

16. As per claim 17, Porras discloses sending requests from the control center to gateways and/or data collectors for requests to install filters to filter out attacking traffic(see col. 5, lines 4-22, col. 13, lines 60-65, col. 14, lines 1-7).

17. As per claim 18, it is rejected under the same basis as claim 1.

18. As per claim 19, it is rejected under the same basis as claim 12.

19. As per claim 20, Porras discloses determine a filtering process to eliminate the malicious traffic from entering the victim data center; and aggregate traffic information and coordinating measures to locate and block the sources of an attack (col. 5, lines 4-22, col. 13, lines 60-65, col. 14, lines 1-7).

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 7-8, 14, are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras in view of Hill et al.

22. Porras does not disclose classifying attack. However, Hill et al. does disclose classifying attacks(see col. 5, lines 66-67, col. 6, lines 1-18). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Hill et al. classifying attacks within Porras, because classifying attacks displays attack information in a usable and quickly interpretable form to a network manager while minimizing the loading on the computer(see col. 2, lines 45-50 of

Hill et al.). Therefore, by classifying attacks provides a network manager with knowledge of the severity and overall nature of the attack(see col. 2, lines 53-60 of Hill et al.).

23. As per claims 7, 14, Porras discloses wherein the analysis process classifies attacks and determines a response based on the class of attack(see col. 2, lines 63-67, col. 3, lines 1-17).

24. As per claim 8, Hill et al. discloses wherein the classes of attack are denoted as low-grade with spoofing, low-grade without spoofing and high-grade whether spoofing or non-spoofing(see fig. 3, sheet 3, fig. 7, sheet 6).

Response to Amendment

24. The Applicant states that Porras does not disclose a control center that is coupled to a network including a communication device to receive data from a plurality of monitors, dispersed thorough the network, with the monitors sending data collected from the network over a hardened, redundant network. The Examiner disagrees with the Applicant. The control center of Porras is the resolver(see fig. 2, sheet 2). The resolver has a plurality of monitors, where the monitors can analyze event records that form an event stream(see col. 4, lines 48-65, col. 8, lines 66-67). The Applicant states that the central controller is part of a larger system. The Applicant seems to be interpreting specific features of the specification into the claims. However, the claims are interpreted broadly. This point is moot, because it is not claimed.

25. The Applicant states that Porras does not disclose a plurality of monitors over a hardened, redundant network. The Examiner disagrees. Porras discloses a monitor collects event reports from different monitors and can correlate activity to identify attacks causing disturbances in more than one network entity (see col. 2, lines 57-60). The network entity of Porras is

VPN(virtual private network)(col. 2, lines 8-10). Therefore, Porras discloses a hardened redundant network.

26. The Applicant states that Porras does not disclose a system that includes a central controller to coordinate thwarting attacks on a victim data center with the central controller system. The Examiner disagrees. The victim data center of Porras is the domain. Porras discloses a domain includes one or more computers offering local services (see col. 3, lines 16-31). Porras discloses domain monitors that perform surveillance over all or part of the domain (see col. 3, lines 66-67). Porras discloses that the domain monitors correlate intrusion reports disseminated by individual monitors (see col. 3, lines 66-67, col. 4, lines 1-3). Porras also, discloses a monitor includes a resolver(see col. 4, lines 55-57), and as stated above the resolver is the central controller.

27. The controller center of Porras does collect statistical information and aggregate traffic, because Porras discloses a resolver that has a plurality of monitors, and these monitors have analysis engines that collect and aggregate traffic(see col. 2, lines 36-53, col. 4, lines 48-60).

28. The Examiner disagrees with the Applicant that the control center is not a hardened site of Porras, because the control center is on the VPN network; therefore, it is a hardened site(see col. 2, lines 54-60).

FINAL ACTION

29. THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jenise E Jackson whose telephone number is (703) 306-0426. The examiner can normally be reached on M-Th (6:00 a.m. - 3:30 p.m.) alternate Friday's.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

September 29, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100